Acta Univ. Sapientiae, Informatica, **4,** 1 (2012) 33–47

Counting (k, l)-sumsets in groups of prime order

Vahe SARGSYAN
Moscow State University
email: vahe_sargsyan@ymail.com

Abstract. A subset A of a group $\mathbf{G}$ is called (k, l)-*sumset*, if $A = kB - lB$ for some $B \subseteq \mathbf{G}$, where $kB - lB = \{x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l} : x_1, \ldots, x_{k+l} \in B\}$. Upper and lower bounds for the number (k, l)-sumsets in groups of prime order are provided.

1 Introduction

Let p be a prime number and k, l be nonnegative integers with $k+l \geq 2$. Write $\mathbf{Z}_p$ for the group of residues modulo p. A subset $A \subseteq \mathbf{Z}_p$ is called (k, l)-*sumset*, if $A = kB - lB$ for some $B \subseteq \mathbf{Z}_p$, where $kB - lB = \{x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l} : x_1, \ldots, x_{k+l} \in B\}$. Write $\mathbf{SS}_{k,l}(\mathbf{Z}_p)$ for the collection of (k, l)-sumsets in $\mathbf{Z}_p$.

B. Green and I. Ruzsa in [1] proved

$$p^2 2^{p/3} \ll |\mathbf{SS}_{2,0}(\mathbf{Z}_p)| \leq 2^{p/3+\theta(p)}$$

where $\theta(p)/p \to 0$ as $p \to \infty$ and $\theta(p) \ll p(\log\log p)^{2/3}(\log p)^{-1/9}$ (hereafter logarithms are to base two).

The aim of this work is to obtain bounds for the number $|\mathbf{SS}_{k,l}(\mathbf{Z}_p)|$. We prove

Theorem 1 *Let p be a prime number and k,l be nonnegative integers with $k + l \geq 2$. Then there exists a positive constant $C_{k,l}$ such that*

$$C_{k,l} 2^{p/(2(k+l)-1)} \leq |SS_{k,l}(Z_p)| \leq 2^{(p/(k+l+1))+(k+l-2)+o(p)}. \tag{1}$$

Computing Classification System 1998: G.2.1
Mathematics Subject Classification 2010: 68R05
Key words and phrases: sumset, characteristic function, partition, glanular set

2 Definitions and auxiliary results

Let $\mathbf{R}$ be the set of real numbers, $f_i : \mathbf{Z}_p \to \mathbf{R}$, $i = 1, \dots, m$, and $x \in \mathbf{Z}_p$. We set

$$(f_1 * \cdots * f_m)(x) =$$
$$= \sum_{x_1 \in \mathbf{Z}_p} \cdots \sum_{x_{m-1} \in \mathbf{Z}_p} f_1(x_1) \dots f_{m-1}(x_{m-1}) f_m(x - x_1 - \cdots - x_{m-1}) \qquad (2)$$

and

$$\widehat{f}(x) = \sum_{y \in \mathbf{Z}_p} f(y) e^{2\pi i \frac{xy}{p}}.$$

The function $\widehat{f}(x)$ is called *Fourier transform* of f.

Lemma 2 *We have*

$$(f_1 \widehat{* \cdots *} f_m)(x) = \widehat{f_1}(x) \dots \widehat{f_m}(x). \qquad (3)$$

Proof. By definition

$$(f_1 \widehat{* \cdots *} f_m)(x) = \sum_{y \in \mathbf{Z}_p} (f_1 * \cdots * f_m)(y) e^{2\pi i \frac{yx}{p}} =$$
$$= \sum_{y \in \mathbf{Z}_p} \sum_{y_1 \in \mathbf{Z}_p} \cdots \sum_{y_{m-1} \in \mathbf{Z}_p} f_1(y_1) \dots f_{m-1}(y_{m-1}) \times$$
$$\times f_m(y - y_1 - \cdots - y_{m-1}) \cdot e^{2\pi i \frac{y_1 x}{p}} \dots e^{2\pi i \frac{y_{m-1} x}{p}} \cdot e^{2\pi i \frac{(y - y_1 - \cdots - y_{m-1})x}{p}} =$$
$$= \sum_{y_1 \in \mathbf{Z}_p} f_1(y_1) \cdot e^{2\pi i \frac{y_1 x}{p}} \cdots \sum_{y_{m-1} \in \mathbf{Z}_p} f_{m-1}(y_{m-1}) \cdot e^{2\pi i \frac{y_{m-1} x}{p}} \times$$
$$\times \sum_{y \in \mathbf{Z}_p} f_m(y - y_1 - \cdots - y_{m-1}) \cdot e^{2\pi i \frac{(y - y_1 - \cdots - y_{m-1})x}{p}} = \widehat{f_1}(x) \dots \widehat{f_m}(x).$$

□

Denote the characteristic function of a set A by $\chi_A(x)$. Let $A_1, \dots, A_m$ be non-empty subsets of $\mathbf{Z}_p$. Then $(\chi_{A_1} * \cdots * \chi_{A_m})(x)$ will be the number of vectors $(x_1, \dots, x_m) \in A_1 \times \cdots \times A_m$ such that $x \equiv x_1 + \cdots + x_m \pmod p$. Set $A_1 + \cdots + A_m = \{x_1 + \cdots + x_m \pmod p : x_1 \in A_1, \dots, x_m \in A_m\}$. We define $S_{h,m}(A_1, \dots, A_m) = \{x \in \mathbf{Z}_p : (\chi_{A_1} * \cdots * \chi_{A_m})(x) \geq h\}$, where $h > 0$. Further, for any integer i and any $A \subseteq \mathbf{Z}_p$ denote the set $\underbrace{A + \cdots + A}_{i}$ by iA, and the set $\{p - x : x \in A\}$ by $-A$.

Theorem 3 (Cauchy-Davenport, [2]). *Let $A_1, \dots, A_m$ be non-empty subsets of $\boldsymbol{Z}_p$. Then* $|A_1 + \cdots + A_m| \geq \min(p, |A_1| + \cdots + |A_m| - (m-1))$.

Theorem 4 (Pollard, [3]). *Let A_1, A_2 be non-empty subsets of $\boldsymbol{Z}_p$. Then*

$$|S_{1,2}(A_1, A_2)| + \cdots + |S_{t,2}(A_1, A_2)| \geq t \min(p, |A_1| + |A_2| - t),$$

where $t \leq \min(|A_1|, |A_2|)$.

Theorems 3, 4 imply the following two statements.

Lemma 5 *Let $A_1, \dots, A_m$ non-empty subsets of $\boldsymbol{Z}_p$. Then*

$$|S_{1,m}(A_1, \dots, A_m)| + \cdots + |S_{t,m}(A_1, \dots, A_m)| \geq$$

$$\geq t \min(p, |A_1| + \cdots + |A_m| - t - m + 2),$$

where $t \leq \min(|A_1|, \dots, |A_m|)$.

Proof. Without loss of generality we assume $|A_1| = \min(|A_1|, \dots, |A_m|)$. By Theorem 4 we have

$$|S_{1,2}(A_1, (A_2 + \cdots + A_m))| + \cdots + |S_{t,2}(A_1, (A_2 + \cdots + A_m))| \geq$$

$$\geq t \min(p, |A_1| + |A_2 + \cdots + A_m| - t), \tag{4}$$

where $t \leq |A_1|$.
On the other hand by Theorem 3 we have

$$|A_2 + \cdots + A_m| \geq \min(p, |A_2| + \cdots + |A_m| - (m-2)). \tag{5}$$

Substituting (5) in (4), we obtain

$$|S_{1,m}(A_1, \dots, A_m)| + \cdots + |S_{t,m}(A_1, \dots, A_m)| \geq$$

$$\geq |S_{1,2}(A_1, (A_2 + \cdots + A_m))| + \cdots + |S_{t,2}(A_1, (A_2 + \dots + A_m))| \geq$$

$$\geq t \min(p, |A_1| + \cdots + |A_m| - t - m + 2).$$

□

Lemma 6 *Let $A_1, \dots, A_m$ be non-empty subsets of $\boldsymbol{Z}_p$ and $h \leq \min(|A_1|, \dots, |A_m|)$. Then*

$$|S_{h,m}(A_1, \dots, A_m)| \geq \min(p, |A_1| + \cdots + |A_m| - m + 2) - 2(hp)^{1/2}.$$

Proof. Note that $|S_{i,m}(A_1,\dots,A_m)| \geq |S_{j,m}(A_1,\dots,A_m)|$ for $i \leq j$. Choose $h \leq t \leq \min(|A_1|,\dots,|A_m|)$. By Lemma 5 we have

$$t\min(p, |A_1| + \cdots + |A_m| - t - m + 2) \leq$$
$$\leq |S_{1,m}(A_1,\dots,A_m)| + \cdots + |S_{t,m}(A_1,\dots,A_m)| \leq$$
$$\leq hp + t|S_{h,m}(A_1,\dots,A_m)|.$$

Putting $t = (hp)^{1/2}$, we get

$$\min(p, |A_1| + \cdots + |A_m| - m + 2) - 2(hp)^{1/2} \leq$$
$$\leq \min(p, |A_1| + \cdots + |A_m| - m - (hp)^{1/2} + 2) - (hp)^{1/2} \leq$$
$$\leq |S_{h,m}(A_1,\dots,A_m)|.$$

□

Lemma 7 *Set* $\boldsymbol{T}_{r,s}(\boldsymbol{Z}_p) = \{A \subset \boldsymbol{Z}_p : |A| \leq p/(r+1)s\}$. *Then there exists* s *such that*

$$|\boldsymbol{T}_{r,s}(\boldsymbol{Z}_p)| \leq 2^{p/(r+1)}. \tag{6}$$

Proof. Let n, m be positive integers, $1 \leq m \leq n$. Then (see Lemma 6.8, [4])

$$\sum_{0\leq i\leq m} \binom{n}{i} \leq \left(\frac{en}{m}\right)^m. \tag{7}$$

We choose s such that

$$es(r+1) \leq 2^s. \tag{8}$$

Then by (7) we have (putting $n = p$ and $m = p/(r+1)s$)

$$|\mathbf{T}_{r,s}(\mathbf{Z}_p)| = \sum_{0\leq i\leq p/(r+1)s} \binom{p}{i} \leq (es(r+1))^{p/(r+1)s} \leq (2^s)^{p/(r+1)s} = 2^{p/(r+1)}.$$

□

Let L be a positive integer. For each $y \in \{0,\dots,p-1\}$ we define a partition $\mathbf{R}_{y,L}$ of $\mathbf{Z}_p$ on the intervals of the form $J_i^y = \{(iL+1+y) \pmod p, \dots, ((i+1)L+y) \pmod p\}$, $0 \leq i \leq \lfloor p/L \rfloor - 1$. All intervals are J_i^y of $\mathbf{R}_{y,L}$ have length L, and the set $J_y = \mathbf{Z}_p \setminus \bigcup_i J_i^y$ has cardinality $p - L\lfloor p/L \rfloor < L$. The set J_y is called *remainder* partition $\mathbf{R}_{y,L}$. In what follows we fix $y \in \{0,\dots,p-1\}$ and consider the corresponding partition $\mathbf{R}_{y,L}$. For every $A \subseteq \mathbf{Z}_p$ and any integer d define $d \star A = \{da \pmod p : a \in A\}$. The set $d \star A$ is called *dilation* of A. The set $A \subseteq \mathbf{Z}_p$ is called L-*granular* (see [1]), if some dilation of A is a union of some of the intervals J_i^y (other than remainder). We denote the family of L-granular subsets of $\mathbf{Z}_p$ by $\mathbf{G}_L(\mathbf{Z}_p)$.

Lemma 8 *We have*

$$|\boldsymbol{G}_L(\boldsymbol{Z}_p)| \le p2^{p/L}. \tag{9}$$

Proof. Denote the number of subsets of intervals (other than remainder) of the partition $R_{y,L}$ of $\mathbf{Z}_p$ by $g(R_{y,L})$, and the number of different partitions $R_{y,L}$ of $\mathbf{Z}_p$ by $r(L)$. It is obvious that

$$|\mathbf{G}_L(\mathbf{Z}_p)| \le g(R_{y,L})r(L). \tag{10}$$

Note that the number of intervals (other than remainder) of the partition $\mathbf{R}_{y,L}$ of $\mathbf{Z}_p$ is equal to $\lfloor p/L \rfloor$, and the number of different partitions $\mathbf{R}_{y,L}$ of $\mathbf{Z}_p$ is at most p. This and (10) imply the inequality (9). $\square$

Lemma 9 *Let $A \subseteq \boldsymbol{Z}_p$ have size αp, and let $\varepsilon_1, \varepsilon_2, \varepsilon_3$ be positive real numbers and $L > 0$, k, l be nonnegative integers satisfying $k + l \ge 2$. Suppose that*

$$p > (\sqrt{8(k+l)}L)^{4^{2(k+l)}\alpha^{2(k+l-1)}\varepsilon_1^{-2(k+l)}\varepsilon_2^{-2(k+l-1)}\varepsilon_3^{-1}}. \tag{11}$$

Then there exists a set $A' \subseteq \boldsymbol{Z}_p$ with the following properties:
(i) A' *is* L*-granular;*
(ii) $|A \setminus A'| \le \varepsilon_1 p$;
(iii) *the set* $kA - lA$ *contains all* $x \in \boldsymbol{Z}_p$ *for which* $(\underbrace{\chi_{A'} * \cdots * \chi_{A'}}_{k} * \underbrace{\chi_{-A'} * \cdots * \chi_{-A'}}_{l})(x) \ge (\varepsilon_2 p)^{k+l-1}$, *with at most* $\varepsilon_3 p$ *exceptions.*

Proof. Let $h \in \{0, \dots, p-1\}$, and $\mathbf{R}_{h,L}$ be partition of $\mathbf{Z}_p$.

(i) For given set $A \subset \mathbf{Z}_p$ we define $A' \subset \mathbf{Z}_p$ as the union of intervals J_i^h of the partition $\mathbf{R}_{h,L}$, such that $|A \cap J_i^h| \ge \varepsilon_1 L/2$. From the definition it follows that A' is L-granular. It is easy to see that $(-A)' = -(A')$.

(ii) Let $x \in A \setminus A'$. Then either $x \in J_h$ or $x \in A \cap J_i^h$, $(i = 0, \dots, \lfloor p/L \rfloor - 1)$, and $|A \cap J_i^h| \le \varepsilon_1 L/2$. In the first case we have $|J_h| < L$, and inequality (11) implies $L \le \varepsilon_1 p/2$. Thus,

$$|A \setminus A'| \le \frac{\varepsilon_1 L}{2} \cdot \frac{p}{L} + L \le \varepsilon_1 p.$$

(iii) Let $\widehat{\chi_A}(x)$ be the Fourier transform of the characteristic function χ_A of A, so that

$$\widehat{\chi_A}(x) = \sum_{y \in \mathbf{Z}_p} \chi_A(y) e^{2\pi i \frac{yx}{p}} = \sum_{y \in A} e^{2\pi i \frac{yx}{p}}$$

for all $x \in \mathbf{Z}_p$. Take $\delta = 4^{-(k+l)}\varepsilon_1^{k+l}\varepsilon_2^{k+l-1}\varepsilon_3^{1/2}\alpha^{-(k+l)+3/2}$, where $\varepsilon_1, \varepsilon_2$ and ε_3 are from inequality (11). Set $\mathbf{D} = \{x \neq 0 : |\widehat{\chi_A}(x)| \geq \delta p\}$. We define the function $f(x)$ as follows:

$$f(x) = \frac{1}{2L-1}\sum_{j=-(L-1)}^{L-1} e^{2\pi i \frac{jqx}{p}}.$$

In the future we will show that there exists $q \in \mathbf{Z}_p \setminus \{0\}$ such that for all $x \in \mathbf{Z}_p$ it holds

$$|\widehat{\chi_A}(x)||1 - f^{k+l}(x)| \leq \delta p. \tag{12}$$

The inequality (12) obviously holds for the case $x = 0$, since $f(0) = 1$, as well as for the case $|\widehat{\chi_A}(x)| \leq \delta p$, since $f(x) \in [-1, 1]$. Thus, it remains to show the existence of q such that the inequality (12) holds for all $x \in \mathbf{D}$. First we estimate the value of $1-f(x)$. Denote by $\langle x \rangle$ the distance from x to the nearest integer. We use the fact that $1 - \cos(2\pi x) \leq 2\pi^2\langle x\rangle^2$. Then

$$1 - f(x) = \frac{2}{2L-1}\sum_{j=1}^{L-1}\left(1 - \cos\frac{2\pi jqx}{p}\right) \leq \frac{4\pi^2}{2L-1}\sum_{j=1}^{L-1}\left\langle\frac{jqx}{p}\right\rangle^2 \leq$$

$$\leq \frac{4\pi^2}{2L-1}\left\langle\frac{qx}{p}\right\rangle^2\sum_{j=1}^{L-1} j^2 \leq \frac{2\pi^2L^2}{3}\left\langle\frac{qx}{p}\right\rangle^2. \tag{13}$$

Recall that for $|x| \leq 1$

$$1 - x^m = (1-x)(1 + x + x^2 + \cdots + x^{m-1}) \leq m(1-x). \tag{14}$$

From (13) and (14) it follows

$$|\widehat{\chi_A}(x)||1 - f^{k+l}(x)| \leq (k+l)|\widehat{\chi_A}(x)||1 - f(x)| \leq 8(k+l)L^2\langle qx/p\rangle^2|\widehat{\chi_A}(x)|.$$

Note that if the inequality

$$\left\langle\frac{qx}{p}\right\rangle \leq \frac{1}{\sqrt{8(k+l)}L}\left(\frac{\delta p}{|\widehat{\chi_A}(x)|}\right)^{1/2} \tag{15}$$

holds for some $q \in \mathbf{Z}_p \setminus \{0\}$ and for all $x \in \mathbf{D}$ then the inequality (12) also holds. Now we will prove that such q exists. By definition, we have

$$\langle qx/p\rangle = \min\{(qx \pmod p)/p, (p - qx \pmod p)/p\}.$$

Set $|\mathbf{D}| = d$, $\mathbf{D} = \{r_1, \dots, r_d\}$. We denote $a_i = (1/\sqrt{8(k+l)}L)(\delta p/|\widehat{\chi_A}(r_i)|)^{1/2}$. Then the inequality (15) can be rewritten as

$$\min\{qr_i \pmod p, p - qr_i \pmod p\} \le pa_i, \quad \text{where} \quad i = 1, \dots, d. \tag{16}$$

Denote the set $\{(x_1, \dots, x_d) : x_1, \dots, x_d \in \mathbf{Z}_p\}$ by $\mathbf{Z}_p^d$. We split $\mathbf{Z}_p^d$ on disjoint subsets

$$\mathbf{Z}_p^d = \bigcup_{(i_1,\dots,i_d)} \mathbf{Q}_{i_1,\dots,i_d},$$

where

$$\mathbf{Q}_{i_1,\dots,i_d} = \{(x_1, \dots, x_d) : i_j p a_j < x_j \le (i_j + 1) p a_j, j = 1, \dots, d\}.$$

Let μ_d be number of different sets of $\mathbf{Q}_{i_1,\dots,i_d}$. Using the fact that $0 \le i_j \le 1/a_j - 1$, $j = 1, \dots, d$, we have

$$\mu_d \le \prod_{i=1}^{d} \frac{1}{a_i}.$$

Let us consider the following $p-1$ elements of $\mathbf{Z}_p^d$:

$$(qr_1 \pmod p), \dots, qr_d \pmod p)), \quad \text{where} \ r_1, \dots, r_d \in \mathbf{D}, \quad q = 1, \dots, p-1.$$

We show that if

$$p > \prod_{i=1}^{d} \frac{1}{a_i}, \tag{17}$$

then there exists q such that for all $r_i \in \mathbf{D}$, $i = 1, \dots, d$, the inequality (16) holds. We consider two cases:
(A) If $\mu_d = p - 1$, then we take $q = q_0$, where $q_0 \in \mathbf{Z}_p \setminus \{0\}$ such that
$(q_0 r_1 \pmod p), \dots, q_0 r_d \pmod p)) \in \mathbf{Q}_{0,\dots,0}$.
(B) If $\mu_d < p-1$, then by pigeonhole principle, there are q_1, $q_2 \in \mathbf{Z}_p \setminus \{0\}$ such that the vectors $(q_1 r_1 \pmod p), \dots, q_1 r_d \pmod p))$ and $(q_2 r_1 \pmod p), \dots, q_2 r_d \pmod p))$ belong to the same set of $\mathbf{Q}_{i_1,\dots,i_d}$. Obviously, when $q = q_1 - q_2$ the inequality (16) holds.

We now show that inequality (17) is a consequence of (11). Indeed, by the Parseval's identity, we have

$$p^{-1}\left(\sum_{x\in\mathbf{D}} |\widehat{\chi_A}(x)|^2 + \sum_{x\in\mathbf{Z}_p\setminus\mathbf{D}} |\widehat{\chi_A}(x)|^2\right) = \sum_{x\in\mathbf{Z}_p} |\chi_A(x)|^2 = \alpha p. \tag{18}$$

From (18) it follows
$$\sum_{x\in\mathbf{D}} |\widehat{\chi_A}(x)|^2 \le \alpha p^2. \tag{19}$$
From (19) and the arithmetic and geometric mean inequality, we get
$$\left(\prod_{x\in\mathbf{D}} |\widehat{\chi_A}(x)|^2\right)^{1/d} \le \frac{1}{d}\sum_{x\in\mathbf{D}} |\widehat{\chi_A}(x)|^2 \le \frac{\alpha p^2}{d}.$$
i.e.
$$\prod_{x\in\mathbf{D}} |\widehat{\chi_A}(x)| \le \left(\frac{\alpha p^2}{d}\right)^{d/2}. \tag{20}$$
From (20) we get
$$(\sqrt{8(k+l)}L)^d \left(\prod_{x\in\mathbf{D}} \frac{|\widehat{\chi_A}(x)|}{\delta p}\right)^{1/2} \le (\sqrt{8(k+l)}L\alpha^{1/4}\delta^{-1/2}d^{-1/4})^d. \tag{21}$$
It is easy to see that the right-hand side of (21) is an increasing function of d in the range $d < 64(k+l)^2L^4\alpha/\delta^2 e$.
On the other hand, from (19) we have $d\delta^2p^2 \le \alpha p^2$. Hence, $d \le \alpha/\delta^2$. Consequently
$$(\sqrt{8(k+l)}L\alpha^{1/4}\delta^{-1/2}d^{-1/4})^d \le (\sqrt{8(k+l)}L)^{\alpha/\delta^2}.$$
Recall that $\delta = 4^{-(k+l)}\varepsilon_1^{k+l}\varepsilon_2^{k+l-1}\varepsilon_3^{1/2}\alpha^{-(k+l)+3/2}$. From this it follows that there exists q such that the inequality (12) holds. Moreover, without loss of generality we can assume $q = 1$ (this can be achieved by selecting an appropriate dilation of the set A).

Define two functions $\chi_1(x)$ and $\chi_2(x)$ as follows:
$$\chi_1(x) = \frac{1}{|\mathcal{J}|}(\chi_A * \chi_{\mathcal{J}})(x),$$
$$\chi_2(x) = \frac{1}{|\mathcal{J}|}(\chi_{-A} * \chi_{\mathcal{J}})(x),$$
where $\mathcal{J} = \{-(L-1),\dots,L-1\}$. From (2) it follows that
$$\chi_1(x) = \frac{1}{|\mathcal{J}|}|A \cap (\mathcal{J} + x)|, \tag{22}$$

$$\chi_2(x) = \frac{1}{|\mathcal{J}|}|(-A)\cap(\mathcal{J}+x)|, \tag{23}$$

and from (3) we have $\widehat{\chi_1}(x) = \widehat{\chi_A}(x)f(x)$ and $\widehat{\chi_2}(x) = \widehat{\chi_{-A}}(x)f(x)$. Hence, by Parseval's identity and from (3) we get

$$\sum_{x\in\mathbf{Z}_p}\left|(\underbrace{\chi_A*\cdots*\chi_A}_{k}*\underbrace{\chi_{-A}*\cdots*\chi_{-A}}_{l})(x)-(\underbrace{\chi_1*\cdots*\chi_1}_{k}*\underbrace{\chi_2*\cdots*\chi_2}_{l})(x)\right|^2 =$$

$$=p^{-1}\sum_{x\in\mathbf{Z}_p}\left|(\widehat{\underbrace{\chi_A*\cdots*\chi_A}_{k}*\underbrace{\chi_{-A}*\cdots*\chi_{-A}}_{l}})(x)-(\widehat{\underbrace{\chi_1*\cdots*\chi_1}_{k}*\underbrace{\chi_2*\cdots*\chi_2}_{l}})(x)\right|^2$$

$$= p^{-1}\sum_{x\in\mathbf{Z}_p}\left|\widehat{\chi_A}^k(x)\widehat{\chi_{-A}}^l(x)-\widehat{\chi_1}^k(x)\widehat{\chi_2}^l(x)\right|^2 =$$

$$= p^{-1}\sum_{x\in\mathbf{Z}_p}|\widehat{\chi_A}(x)|^{2k}|\widehat{\chi_{-A}}(x)|^{2l}\left|1-f^{k+l}(x)\right|^2 \le$$

$$\le p^{-1}\left(\sup_{x\in\mathbf{Z}_p}|\widehat{\chi_A}(x)|^{k-1}|\widehat{\chi_{-A}}(x)|^{l}\left|1-f^{k+l}(x)\right|\right)^2\sum_{x\in\mathbf{Z}_p}|\widehat{\chi_A}(x)|^2. \tag{24}$$

We have

$$|\widehat{\chi_A}(x)| = \left|\sum_{y\in\mathbf{Z}_p}\chi_A(y)e^{2\pi i\frac{yx}{p}}\right| = \left|\sum_{y\in A}e^{2\pi i\frac{yx}{p}}\right| \le \sum_{y\in A}\left|e^{2\pi i\frac{yx}{p}}\right| = \alpha p, \tag{25}$$

$$|\widehat{\chi_{-A}}(x)| = \left|\sum_{y\in\mathbf{Z}_p}\chi_{-A}(y)e^{2\pi i\frac{yx}{p}}\right| = \left|\sum_{y\in -A}e^{2\pi i\frac{yx}{p}}\right| \le \sum_{y\in -A}\left|e^{2\pi i\frac{yx}{p}}\right| = \alpha p. \tag{26}$$

From (12), (18), (24), (25) and (26) it follows

$$\sum_{x\in\mathbf{Z}_p}\left|(\underbrace{\chi_A*\cdots*\chi_A}_{k}*\underbrace{\chi_{-A}*\cdots*\chi_{-A}}_{l})(x)-(\underbrace{\chi_1*\cdots*\chi_1}_{k}*\underbrace{\chi_2*\cdots*\chi_2}_{l})(x)\right|^2 \le$$

$$\le\left(\sup_{x\in\mathbf{Z}_p}|\widehat{\chi_A}(x)|\left|1-f^{k+l}(x)\right|\right)^2\alpha^{2(k+l)-3}p^{2(k+l)-3} \le$$

$$\leq \alpha^{2(k+l)-3}\delta^2 p^{2(k+l)-1}. \tag{27}$$

Suppose that $x \in A'$ ($x \in -A'$). Then there exists an interval $\mathcal{I}$ of length L such that $\mathcal{I} \subseteq \{x-(L-1), \dots, x+(L-1)\}$ and $x \in \mathcal{I}$. From definition of A' ($-A'$) it follows that $|\mathcal{I} \cap A| \geq \varepsilon_1 L/2$ ($|\mathcal{I} \cap (-A)| \geq \varepsilon_1 L/2$). From the definition of $\chi_1(x)$ ($\chi_2(x)$) it follows that $\chi_1(x) \geq \varepsilon_1/4$ ($\chi_2(x) \geq \varepsilon_1/4$). Observe, that $\chi_1(x) \geq \varepsilon_1 \chi_{A'}(x)/4$ and $\chi_2(x) \geq \varepsilon_1 \chi_{-A'}(x)/4$ hold for all $x \in \mathbf{Z}_p$. From this and (2) it follows that

$$(\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x) \geq$$

$$\geq \varepsilon_1^{k+l}(\underbrace{\chi_{A'} * \cdots * \chi_{A'}}_{k} * \underbrace{\chi_{-A'} * \cdots * \chi_{-A'}}_{l})(x)/4^{k+l} \tag{28}$$

for all $x \in \mathbf{Z}_p$. In the case

$$(\underbrace{\chi_{A'} * \cdots * \chi_{A'}}_{k} * \underbrace{\chi_{-A'} * \cdots * \chi_{-A'}}_{l})(x) \geq (\varepsilon_2 p)^{k+l-1}, \tag{29}$$

by (28) we have

$$(\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x) \geq \varepsilon_1{}^{k+l}(\varepsilon_2 p)^{k+l-1}/4^{k+l}. \tag{30}$$

Now we show that the number of elements $x \in \mathbf{Z}_p$ such that satisfying (29) and $(\underbrace{\chi_A * \cdots * \chi_A}_{k} * \underbrace{\chi_{-A} * \cdots * \chi_{-A}}_{l})(x) = 0$, does not exceed $\varepsilon_3 p$. Denote the set of such elements by $\mathbf{F}$. Observe, that for every $x \in \mathbf{F}$

$$|(\underbrace{\chi_A * \cdots * \chi_A}_{k} * \underbrace{\chi_{-A} * \cdots * \chi_{-A}}_{l})(x) - (\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x)|^2 \geq$$

$$\geq \frac{\varepsilon_1{}^{2(k+l)}\varepsilon_2{}^{2(k+l-1)}p^{2(k+l-1)}}{4^{2(k+l)}}. \tag{31}$$

By (27) and (31)

$$\alpha^{2(k+l)-3}\delta^2 p^{2(k+l)-1} \geq$$

$$\geq \sum_{x \in \mathbf{Z}_p} \left|(\underbrace{\chi_A * \cdots * \chi_A}_{k} * \underbrace{\chi_{-A} * \cdots * \chi_{-A}}_{l})(x) - (\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x)\right|^2 =$$

$$= \sum_{x\in \mathbf{F}} \left| (\underbrace{\chi_A * \cdots * \chi_A}_{k} * \underbrace{\chi_{-A} * \cdots * \chi_{-A}}_{l})(x) - (\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x) \right|^2 +$$

$$+ \sum_{x\in (\mathbf{Z}_p \setminus \mathbf{F})} \left| (\underbrace{\chi_A * \cdots * \chi_A}_{k} * \underbrace{\chi_{-A} * \cdots * \chi_{-A}}_{l})(x) - (\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x) \right|^2$$

$$\geq |\mathbf{F}| \frac{{\varepsilon_1}^{2(k+l)} {\varepsilon_2}^{2(k+l-1)} p^{2(k+l-1)}}{4^{2(k+l)}} +$$

$$+ \sum_{x\in (\mathbf{Z}_p \setminus \mathbf{F})} \left| (\underbrace{\chi_A * \cdots * \chi_A}_{k} * \underbrace{\chi_{-A} * \cdots * \chi_{-A}}_{l})(x) - (\underbrace{\chi_1 * \cdots * \chi_1}_{k} * \underbrace{\chi_2 * \cdots * \chi_2}_{l})(x) \right|^2 .$$

This implies

$$|\mathbf{F}| \leq \frac{4^{2(k+l)} \alpha^{2(k+l)-3} \delta^2}{{\varepsilon_1}^{2(k+l)} {\varepsilon_2}^{2(k+l-1)}} p \leq \varepsilon_3 p.$$

□

3 The proof of Theorem 1

3.1 The upper bound

Let k,l be nonnegative integers with $k + l \geq 2$. Suppose that s satisfies $es(k + l + 1) \leq 2^s$. We divide a partition of $\mathbf{SS}_{k,l}(\mathbf{Z}_p)$ into two parts:

$$\mathbf{SS}_{k,l}(\mathbf{Z}_p) = \mathbf{SS}'_{k,l,s}(\mathbf{Z}_p) \cup \mathbf{SS}''_{k,l,s}(\mathbf{Z}_p), \tag{32}$$

where

$$\mathbf{SS}'_{k,l,s}(\mathbf{Z}_p) = \{B \in \mathbf{SS}_{k,l}(\mathbf{Z}_p) : B = kA - lA \text{ and } |A| \leq p/(k + l + 1)s\},$$

$$\mathbf{SS}''_{k,l,s}(\mathbf{Z}_p) = \{B \in \mathbf{SS}_{k,l}(\mathbf{Z}_p) : B = kA - lA \text{ and } |A| > p/(k + l + 1)s\}.$$

It is obvious that

$$|\mathbf{SS}_{k,l}(\mathbf{Z}_p)| \leq |\mathbf{SS}'_{k,l,s}(\mathbf{Z}_p)| + |\mathbf{SS}''_{k,l,s}(\mathbf{Z}_p)|. \tag{33}$$

Since every set $A \subseteq \mathbf{Z}_p$ generates one set of the form $kA - lA$ we obtain

$$\left|\mathbf{SS}'_{k,l,s}(\mathbf{Z}_p)\right| \leq |\mathbf{T}_{k+l,s}(\mathbf{Z}_p)| . \tag{34}$$

By (7) and (34) we have

$$\left|\mathbf{SS}'_{k,l,s}(\mathbf{Z}_p)\right| \le 2^{p/(k+l+1)}. \tag{35}$$

Now we prove an upper bound for $|\mathbf{SS}''_{k,l,s}(\mathbf{Z}_p)|$. Suppose that the cardinality of $A \subseteq \mathbf{Z}_p$ is larger than $p/(k+l+1)s$. Let p be a prime number such that for some nonnegative integers $k, l, L > 0$ and positive real numbers $\varepsilon_1, \varepsilon_2$ and ε_3 the condition (11) is fulfilled. By Lemma 9 there exists a subset A' with properties $(i) - (iii)$. We estimate the number of (k,l)-sumsets $kA - lA$ by counting pairs $(A', kA - lA)$.

Now let $A' \in \mathbf{G}_L(\mathbf{Z}_p)$ be given. For any subset $C \subseteq \mathbf{Z}_p$ we denote by $\overline{C}$ the complement of the subset C in $\mathbf{Z}_p$.

If $|A'| \ge p/(k+l+1)$, then from (iii) of Lemma 9 we obtain that $\overline{kA - lA}$ is a subset of the union of the set $\overline{S_{(\varepsilon_2 p)^{k+l-1},k+l}(\underbrace{\chi_{A'},\dots,\chi_{A'}}_{k},\underbrace{\chi_{-A'},\dots,\chi_{-A'}}_{l})}$ and a set of cardinality not exceeding $\varepsilon_3 p$. By Lemma 6 we have

$$|S_{(\varepsilon_2 p)^{k+l-1},k+l}(\underbrace{\chi_{A'},\dots,\chi_{A'}}_{k},\underbrace{\chi_{-A'},\dots,\chi_{-A'}}_{l})| \ge$$

$$\ge \min(p,(k+l)|A'| - (k+l) + 2) - 2((\varepsilon_2 p)^{k+l-1}p)^{1/2}.$$

If $|A'| \ge p/(k+l+1)$, we obtain

$$|\overline{S_{(\varepsilon_2 p)^{k+l-1},k+l}(\underbrace{\chi_{A'},\dots,\chi_{A'}}_{k},\underbrace{\chi_{-A'},\dots,\chi_{-A'}}_{l})}| =$$

$$= p - |S_{(\varepsilon_2 p)^{k+l-1},k+l}(\underbrace{\chi_{A'},\dots,\chi_{A'}}_{k},\underbrace{\chi_{-A'},\dots,\chi_{-A'}}_{l})| \le$$

$$\le p/(k+l+1) + 2\varepsilon_2^{(k+l-1)/2}p^{(k+l)/2} + (k+l-2).$$

It is obvious that for any subset $B \subseteq \mathbf{Z}_p$ the set $kB - lB$ uniquely determines the set $\overline{kB - lB}$. From above it follows that the number of choices $kA - lA$ for given A' of cardinality exceeding $p/(k+l+1)$, is at most

$$2^{p/(k+l+1)+(k+l-2)+(2\varepsilon_2^{(k+l-1)/2}p^{(k+l-2)/2}+\varepsilon_3)p}. \tag{36}$$

If $|A'| < p/(k+l+1)$, then by (i) of Lemma 9 we have $|A \setminus A'| \le \varepsilon_1 p$. This implies that $|A| \le |A'| + \varepsilon_1 p$. Since every set $A \subseteq \mathbf{Z}_p$ generates exactly one set of form $kA - lA$, we obtain that the number of choices $kA - lA$ for given A' of cardinality not exceeding $p/(k+l+1)$, is at most

$$2^{p/(k+l+1)+\varepsilon_1 p}. \tag{37}$$

From (36), (37), Lemma 8 by applying Lemma 9 with parameters $\varepsilon_1 = \varepsilon_3 = \varepsilon$, $L = 1 + \lfloor 1/\varepsilon \rfloor$ and $\varepsilon_2 = \varepsilon^{2/(k+l-1)} p^{(2-k-l)/(k+l-1)}$, we obtain

$$|\mathbf{SS}''_{k,l,s}(\mathbf{Z}_p)| \le 2^{(p/(k+l+1))+(k+l-2)+o(p)}. \tag{38}$$

From (33), (35) and (38) it follows that

$$|\mathbf{SS}_{k,l}(\mathbf{Z}_p)| \le 2^{p/(k+l+1)} + 2^{(p/(k+l+1))+(k+l-2)+o(p)} = 2^{(p/(k+l+1))+(k+l-2)+o(p)}.$$

3.2 The lower bound

Set $\mathbf{SS}_{k,l}(\mathbf{Z}_p, \mathbb{P}) = \{A : \mathbb{P} \subseteq A,\ A \in \mathbf{SS}_{k,l}(\mathbf{Z}_p)\}$ and $L = \lfloor p/(2(k+l)-1) \rfloor - 1$.

Lemma 10 *Let* k,l *be nonnegative integers with* $k+l \ge 2$, *and let* $\mathbb{P} \subseteq \boldsymbol{Z}_p$ *be arbitrary arithmetic progression of length* $(k+l)(L-1)+1$. *Then there exists a positive constant* $\boldsymbol{C}_{k,l}$ *such that*

$$|\boldsymbol{SS}_{k,l}(\boldsymbol{Z}_p, \mathbb{P})| \ge \boldsymbol{C}_{k,l} 2^{p/(2(k+l)-1)}.$$

Proof. Without loss of generality we assume $\mathbb{P} = \{k - lL, \dots, kL - l\}$. All of our sets will be of the form

$$A = A(B) = k(B \cup \{-(2L+1), 2L+1\}) - l(B \cup \{-(2L+1), 2L+1\}),$$

where $B \subseteq \{-L, -L+1, \dots, L\}$ and $-B = B$. It is easy to see that different sets $B \subseteq \{-L, -L+1, \dots, L\}$ generate different sets $A(B)$.

Set $N_{k,l} = \lceil \log(8(k+l)^2)/\log(4/3) \rceil$ and

$$X = \{0, 1, \dots, N_{k,l}\} \cup \bigcup_{i=1}^{k+l-1} (\lfloor (i+1)L/(k+l) \rfloor - N_{k,l}, \dots, \lceil (i+1)L/(k+l) \rceil).$$

We define the set $B \subseteq \{-L, -L+1, \dots, L\}$ as follows:

$$B = B(C) = -C \cup C \cup X \cup -X,$$

where elements of the set C are picked from the set $\{1, \dots, L\} \setminus X$ randomly, independently, with probability $1/2$. Set

$$Y = \{0\} \cup \{k+l, \dots, (k+l)N_{k,l}\} \cup \bigcup_{i=1}^{k+l-1} \{(i+1)L - (k+l)N_{k,l}, \dots, (i+1)L\}.$$

It is obvious that $-Y \cup Y \subseteq kB - lB$. If $x \notin kB - lB$, then in the representation x in the form $x = x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l}$, there exists at least one x_i ($i \in \{1, \ldots, k+l\}$) such that $x_i \notin B$. Set

$$\mathcal{Q}(x) = \{(x_1, \ldots, x_{k+l}) : x = \sum_{i=1}^{k} x_i - \sum_{j=k+1}^{k+l} x_j, x_1, \ldots, x_{k+l} \in \{-L, \ldots, L\}\},$$

and suppose that $|\mathcal{Q}(x)| = q$.

We say that the vectors $(x_1, \ldots, x_{k+l})$ and $(y_1, \ldots, y_{k+l})$ do not intersect, if $\{x_1, \ldots, x_{k+l}\} \cap \{y_1, \ldots, y_{k+l}\} = \emptyset$.

Set $\mathcal{R}_0 = \{(k+l)N_{k,l} + 1, \ldots, L\}$. We show that for every $x \in -\mathcal{R}_0 \cup \mathcal{R}_0$ the following inequality

$$\mathbf{Pr}(x \notin kB - lB) \le \left(\frac{3}{4}\right)^{\left\lfloor \frac{|x|}{k+l} \right\rfloor} \tag{39}$$

holds. We have

$$\begin{aligned}
&\mathbf{Pr}(x \notin kB - lB) = \\
&= \mathbf{Pr}((x_1^1 + \cdots + x_k^1 - x_{k+1}^1 - \cdots - x_{k+l}^1 \notin kB - lB) \& \ldots \\
&\ldots \& (x_1^q + \cdots + x_k^q - x_{k+1}^q - \cdots - x_{k+l}^q \notin kB - lB)) \le \\
&\le \mathbf{Pr}((x_1^{11} + \cdots + x_k^{11} - x_{k+1}^{11} - \cdots - x_{k+l}^{11} \notin kB - lB) \& \ldots \\
&\ldots \& (x_1^{1n} + \cdots + x_k^{1n} - x_{k+1}^{1n} - \cdots - x_{k+l}^{1n} \notin kB - lB)) = \\
&= \mathbf{Pr}\left((x_1^{11} \notin B \vee \cdots \vee x_{k+l}^{11} \notin B) \& \ldots \& (x_1^{1n} \notin B \vee \cdots \vee x_{k+l}^{1n} \notin B)\right) = \\
&= \mathbf{Pr}\left((x_1^{11} \notin B) \vee \cdots \vee (x_{k+l}^{11} \notin B)\right) \cdot \ldots \cdot \mathbf{Pr}\left((x_1^{1n} \notin B) \vee \cdots \vee (x_{k+l}^{1n} \notin B)\right) = \\
&= \mathbf{Pr}\left(\overline{(x_1^{11} \in B) \& \ldots \& (x_{k+l}^{11} \in B)}\right) \times \ldots \\
&\cdots \times \mathbf{Pr}\left(\overline{(x_1^{1n} \in B) \& \ldots \& (x_{k+l}^{1n} \in B)}\right) = \\
&= \left(1 - \mathbf{Pr}\left((x_1^{11} \in B) \& \ldots \& (x_{k+l}^{11} \in B)\right)\right) \times \ldots \\
&\cdots \times \left(1 - \mathbf{Pr}\left((x_1^{1n} \in B) \& \ldots \& (x_{k+l}^{1n} \in B)\right)\right),
\end{aligned} \tag{40}$$

where the vectors $(x_1^i, \ldots, x_{k+l}^i) \in \mathcal{Q}(x), i = 1, \ldots, q$, and the vectors $(x_1^{1j}, \ldots, x_{k+l}^{1j})$, $j = 1, \ldots, n \le q$, are pairwise disjoint.

Note that the vectors $(x-i(k+l-1), \underbrace{i,\dots,i}_{k-1}, \underbrace{-i,\dots,-i}_{l})$ are pairwise disjoint for every $x \in -\mathcal{R}_0$, where $-\lfloor |x|/(k+l) \rfloor \le i \le -1$, and $x \in \mathcal{R}_0$, where $1 \le i \le \lfloor x/(k+l) \rfloor$. From this and (40) we obtain the inequality (39).

Set $\mathcal{L}_j = \{jL+1,\dots,(j+1)L-(k+l)N_{k,l}-1\}$, $j = 1,\dots,k+l-1$. Similarly to the inequality (39) we have

$$\mathbf{Pr}(x \notin kB - lB) \le \left(\frac{3}{4}\right)^{\left\lfloor \frac{(j+1)L-|x|}{k+l} \right\rfloor}, \tag{41}$$

where $x \in -\mathcal{L}_j \cup \mathcal{L}_j$, $j = 1,\dots,k+l-1$.

From (39) and (41) it is easy to see that

$$\mathbf{Pr}\left(\mathbb{P} \nsubseteq kB - lB\right) \le (k+l) \sum_{x \ge (k+l)N_{k,l}+1} \left(\frac{3}{4}\right)^{\left\lfloor \frac{x}{k+l} \right\rfloor}. \tag{42}$$

Note that if $N_{k,l} \ge \log\left(8(k+l)^2\right)/\log(4/3)$, the right-hand side of (42) does not exceed $1/2$. This leads that there exists at least $2^{L-(k+l)N_{k,l}-1}$ subsets $B \subseteq \{-L,-L+1,\dots,L\}$ such that $\mathbb{P} \subseteq kB - lB$. $\square$

Let k,l be nonnegative integers with $k+l \ge 2$, and let $\mathbb{P} \subseteq \mathbf{Z}_p$ be arbitrary arithmetic progression of length $(k+l)(L-1)+1$. By Lemma 10 we have

$$|SS_{k,l}(\mathbf{Z}_p)| \ge |\mathbf{SS}_{k,l}(\mathbf{Z}_p,\mathbb{P})| \ge \mathbf{C}_{k,l} 2^{p/(2(k+l)-1)}.$$

Acknowledgements

The author expresses his gratitude to his supervisor Prof. A. A. Sapozhenko for the statement of the problem and attention to this work. The research was supported by RFBR project Nr 10-01-00768-a.

References

[1] B. Green, I. Ruzsa, Counting sumsets and sum-free sets modulo a prime, *Studia Sci. Math. Hungarica* **41,** 3 (2004) 285–293. ⇒33, 36

[2] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets.* Vol. 165. Graduate Texts in Mathematics, Springer-Verlag, New York, 1996. ⇒35

[3] J. M. Pollard, A generalization of the theorem of Cauchy and Davenport, *J. London Math. Soc.* **8,** 2 (1974) 460–462. ⇒35

[4] A. A. Sapozhenko, *Dedekind Problem and the Method of Boundary Functionals*, Fizmatlit, Moscow, 2009. ⇒36

Received: March 8, 2012 • Revised: April 16, 2012